Penerapan Analisis Kerentanan XSS dan Rate Limiting pada Situs Web MTsN 3 Negara Menggunakan OWASP ZAP

I.B. Indra Dewangkara[1], K. Satwitri Santi[2], V.A. Putri[3], I.M. Edy Listartha[4]
[1,2,3,4]*Jurusan Teknik Informatika, Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha*
Jl. Udayana No.11, Banjar Tegal, Singaraja, Kabupaten Buleleng, Bali 81116
E-mail : bagus.indra.dewangkara@undiksha.ac.id[1], widya.satwitri@undiksha.ac.id[2], vany@undiksha.ac.id[3], listartha@undiksha.ac.id[4]

Abstract*— Indonesia which has entered the era of digitalization, makes the education sector expected to be able to adapt. Nowadays, learning Online is one of the learning methods in Indonesia. With these conditions and situations, websites have an important role in supporting education in today's digital era. This triggers as need for an analysis of the vulnerability of school websites in Indonesia. The target is to implement this analysis is on Islamic Junior High Scholl of Jembrana website. Cross site scripting (XSS) vulnerability analysis and rate limiting function to prevent hacks that harm to MTs.N 2 Negara website. The application of this analysis is uses a software called OWASP as an supporting media. As the results of the security analysis of Islamic Junior High Scholl of Jembrana website, there are vulnerabilities in rate limiting and XSS analysis experiments that were not found. In addition, there are also solutions to vulnerabilities that exist on Islamic Junior High Scholl of Jembrana website

***Abstrak*— Indonesia yang sudah memasuki era digitalisasi membuat sektor pendidikan diharapkan mampu untuk beradaptasi. Pembelajaran daring kini menjadi salah satu metode pembelajaran di Indonesia. Dengan adanya kondisi dan situasi tersebut, situs web memiliki peran penting dalam penunjang pendidikan di era digital saat ini. Hal tersebut memicu perlunya analisa terhadap kerentanan situs-situs web sekolah yang ada di Indonesia. Target penerapan analisis ini ada pada situs web MTsN 3 Negara. Analisis kerentanan *cross site scripting* (XSS) serta *rate limiting* berfungsi untuk mencegah adanya peretasan yang merugikan situs web MTsN 3 Negara. Penerapan alisis ini menggunakan salah satu perangkat lunak bernama OWASP sebagai media pendukungnya. Adapun hasil dari analisis keamanan situs web MTsN 3 Negara ini terdapat kerentanan pada *rate limiting* serta percobaan analisis *cross-site scripting* (XSS) yang tidak ditemukan. Selain itu, terdapat juga solusi-solusi terhadap kerentanan yang ada pada situs web MTsN 3 Negara.**

***Kata Kunci*— Kerentanan, MTsN 3 Negara, *Rate limiting,* Situs web, XSS.**

I. PENDAHULUAN

Era digitalisasi memaksakan masyarakat untuk mampu hidup dan beradaptasi dengan zamannya. Sebab, masyarakat kini sangat bergantung dengan adanya internet. Situs web adalah salah satu alat yang sering dimanfaatkan oleh masyarakat dalam berbagai jenis pekerjaan. Secara definisi, situs web adalah kumpulan informasi dalam satu halaman serta informasi tersebut harus diakses melalui melalui internet. Masyarakat yang harus membuka serta mengoperasikan situs web memerlukan suatu jembatan yang disebut sebagai peramban.

Dahulu situs web dipergunakan untuk penyebaran informasi belaka. Namun, kini situs web sudah menjadi alat yang dapat mempermudah masyarakat dalam pekerjaannya. Pekerjaan yang dapat dipermudah dengan adanya situs web salah satunya adalah pendidikan. Kini dunia pendidikan sangat membutuhkan adanya situs web mengingat pentingnya penerapan pembelajaran daring sebagai pencegahan penyebaran virus Covid-19.

Namun, pihak pengembang situs web perlu memerhatikan adanya serangan siber yang kini dapat merugikan banyak pihak. Keamanan siber adanya sebuah ancaman kejahatan dalam dunia internet. Situs web sekolah tidak dapat dikatakan aman dari kejahatan siber ini. Maka dari itu, penting untuk pihak tim pengembang situs web agar mampu mengatasi adanya serang siber. Apalagi, pada situs web sekolah yang berisikan fitur-fitur rentan seperti informasi siswa, informasi guru, data *login, e-learning,* dan sebagainya sangat rentan menjadi bidikan para penjahat di dunia siber.

Berbicara mengenai keamanan siber, tentu diperlukan adanya uji kerentanan pada situs web guna mencegah adanya hal-hal yang tidak diinginkan. Keamanan yang cukup rentan menjadi serangan penjahat di dunia siber adalah *cross-site scripting* (XSS) dan *rate limiting*. Pengujian perlu dilakukan oleh tim pengembang, maupun pihak yang peduli dengan adanya kerentanan situs web sekolah.

Di Provinsi Bali, situs web sekolah sudah berkembang begitu pesat semenjak adanya penyebaran virus Covid-19. Pembelajaran yang harus dilakukan secara daring adalah salah satu pemicunya. Salah satu situs web yang menarik untuk dilakukan pengujian adalah situs web miliki MTsN 3 Negara. MTsN 3 Negara adalah sekolah Madrasah sanawiah Negeri yang terletak di Jalan Raya Negara – Gilimanuk, Desa Kaliakah, Kecamatan Melaya, Kabupaten Jembrana. Sekolah ini memiliki situs web yang beralamat domain di mtsnnegarabali.sch.id. Situs web MTSn3 Negara memiliki beberapa fitur, di antara lainnya adalah: 1) *Login;* 2) Ulang tahun siswa; 3) Biodata guru; 4) Berita prestasi; 5) Dan lain-lainMetode Penelitian. Penelitian ini telah menguji bagaimana kerentanan situs web MTSn 3 Negara dari segi *cross-site scripting* (XSS) serta *rate limiting* dengan metode-metode dengan hasil dan pembahasan yang telah dijelaskan lebih lanjut.

II. METODE PENELITIAN

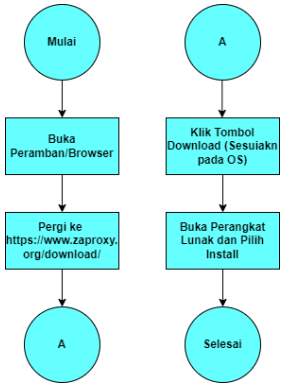
Pada alur proses penelitian ini, terdapat empat tahapan yang disusun secara sistematis. Adapun keempat tahapan tersebut di antara lainnya yakni: 1) Unduh dan Install Perangkat Lunak OWASP ZAP; 2) Uji Kerentanan pada Perangkat Lunak OWASP ZAP; 3) Penyajian Hasil Uji Kerentanan; 4) Penyajian Solusi Terhadap Kerentanan yang Ditemukan. Tahapan-tahapan sistematis pada penelitian keamanan situs web MTsN 3 Negara dapat dilihat pada gambar di bawah ini.

Gambar 1. Tahap-tahap pengujian kerentanan situs web

Dapat diperhatikan pada gambar 1 yang merupakan gambaran dari tahapan-tahapan yang telah diterapkan pada kegiatan analisis kerentanan *cross-site scripting* (XSS) dan *rate limiting* pada situs web MTsN 3 Negara. Pada pengunduhan serta install perangkat lunak OWASP ZAP merupakan langkah pertama yang perlu dilakukan. Setelah itu, pengujian yang pertama dilakukan yakni proses *scanning* pada *tool* ZAP; selanjutnya yakni pengujian kerentanan *cross-site scripting* (XSS) dengan memanfaatkan *payload* XSS; yang terakhir yakni pengujian terhadap *rate limiting* pada fitur login situs web MTsN 3 Negara. Tahap ketiga adalah tahap penyajian hasil uji kerentanan; tahap ini berfokus pada menganalisis hasil dari uji *scanning,* kerentanan *cross-site scripting* (XSS), serta keretanan *rate limiting* yang sudah dilakukan sebelumnya. Tahap yang terakhir adalah penyajian solusi terhadap keretanan yang ditemukan; dengan kata lain tahap ini adalah memberikan solusi-solusi pada kerentanan yang telah ditemukan pada tahap kedua agar mampu meminimalisir kejahatan siber yang tidak diinginkan. Pada masing-masing alur utama tersebut, terdapat lagi alur baru sebagai langkah dari tahap pertama ke tahap yang berikutnya.

A. Tahap Pertama

Pada langkah pertama, yakni unduh dan instalasi perangkat lunak OWASP ZAP merupakan langkah awal yang bisa menjadi paling penting pada penelitian ini. OWASP ZAP merupakan perangkat lunak berbasis desktop yang menyediakan fitur *scanning* kerentanan situs web; serta memberikan tool guna melakukan uji kerentanan *cross-site scripting* (XSS)dan *rate limiting*. Adapun alur pada langkah pertama ini dapat dilihat sebagai berikut.

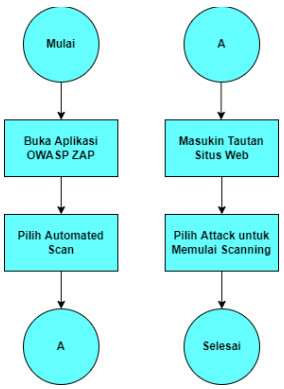


Gambar 2. *Flowchart* tahap unduh dan instalasi

Gambar 2 merupakan *flowchart* atau diagram alir yang menjelaskan bagaiana alur proses pada tahap pertama. Langkah ini cukup umum dan mudah dipahami, tetapi perlu diperhatikan pada proses unduh aplikasi yang harus sesuai dengan sistem operasi.

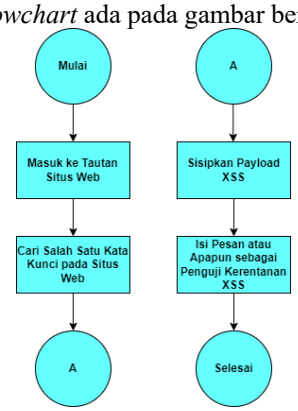
B. Tahap Kedua

Selanjutnya pada langkah kedua, yakni Uji kerentanan pada perangkat lunak. Pada langkah ini sudah masuk ke dalam aktivitas *scanner.* Adapun tiga alur yang dilakukan dalam tahap uji kerentanan ini, di antara lainnya yakni: 1) *Scanning;* 2) Uji Kerentanan *cross-site scripting* (XSS); 3) Uji kerentanan *rate limiting.* Ketiga langkah uji kerentanan juga dapat dilihat pada gambar berikut.



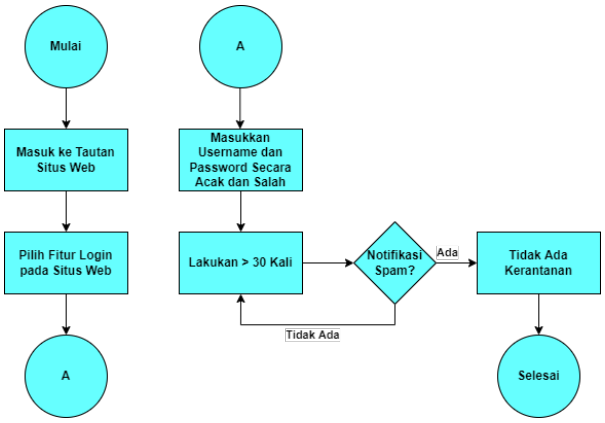
Gambar 3. *Flowchart* tahap *scanning* kerentanan situs web

Gambar 3 menjelaskan bagaimana alur proses dari tahap *scanner*. Selanjutnya, adalah masuk ke proses uji kerentanan XSS dengan *flowchart* ada pada gambar berikut.



Gambar 4. *Flowchart* uji kerentanan XSS pada situs web

Melihat pada gambar 4, uji kerentanan *cross-site scripting* (XSS) tidaklah menggunakan tool dari OWASP ZAP. Namun, pada dasarnya tool OWASP ZAP juga mampu menguji kerentanan XSS. Yang terakhir adalah proses uji kerentanan *rate limiting* yang dapat dilihat pada gambar berikut.



Gambar 5. *Flowchart* uji kerentanan *rate limiting* pada situs web

Langkah terakhir yakni uji kerentanan *rate limiting*, sama dengan uji kerentanan XSS; pada dasarnya pengujian *rate limiting* dapat dilaksanakan melalui tools OWASP ZAP dan juga dilakukan secara manual. Namun, apada penelitian kali ini pelaksanaan uji kerentanan XSS dilakukan secara manual dengan alur proses ada pada gambar 5.

C. *Tahap ketiga*

Tahap ketiga adalah penyajian hasil dari pelaksanaan uji kerentanan situs web berdasarkan *scanning,* kerentanan XSS, dan kerentanan *rate limiting.* Pada tahap ketiga ini, dilaksanakan menyiapkan dokumen-dokumen hasil sebagai metode penelitian. Dokumen hasil uji kerentananakan dijadikan acuan pada tahap selanjutnya.

D. *Tahap Keeempat*

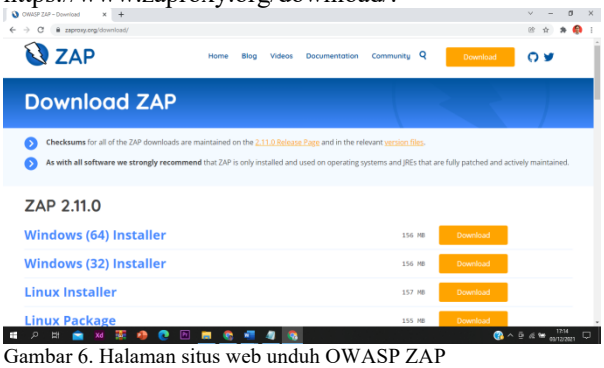
Tahap yang keempat sekaligus yang terakhir adalah penyajian solusi terhadap kerentanan yang ditemukan. Tahap terakhir ini harus berdasarkan pada kerentanan yang ada pada situs web MTsN 3 Negara; baik itu dari segi kerentanan XSS, maupun *rate limiting*.

III. HASIL DAN PEMBAHASAN

Seperti yang sudah dibahas pada metode penelitian, terdapat empat tahapan utama pada penelitian kerentanan *cross-site scripting* (XSS) dan *rate limiting* situs web MTsN 3 Negara. Namun, setelah mengetahui bagaimana alur proses serta metode-metode penelitian yang digunakan, pada bagian ini akan dijelaskan bagaimana hasil serta pembahasan mengenai setiap proses yang ada.

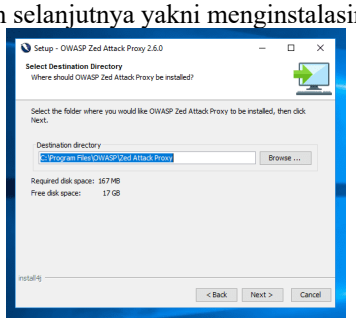
A. *Tahap Pertama*

Hasil pertama adalah hasil dari unduh dan instalasi perangkat lunak OWASP ZAP. Sesuai pada langkah pertama yang harus dilakukan adalah pergi ke tautan situs https://www.zaproxy.org/download/.



Gambar 6. Halaman situs web unduh OWASP ZAP

Perlu diperhatikan untuk sistem operasi yang digunakan. Pada sistem operasi Windows, bit dari Windows juga perlu diperhatikan. Setelah berhasil mengunduh OWASP ZAP, maka langkah selanjutnya yakni menginstalasinya.

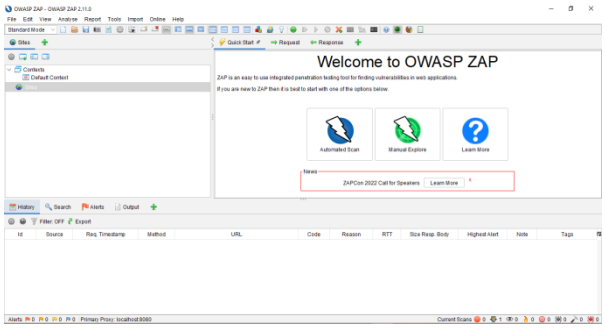


Gambar 7. Instalasi OWASP ZAP

Ikuti arahan yang diberikan oleh sistem sehingga proses instalasi aplikasi berhasil dilakukan. Dengan berakhirnya tahap pertama, maka langkah-langkah berikutnya dapat dilakukan.

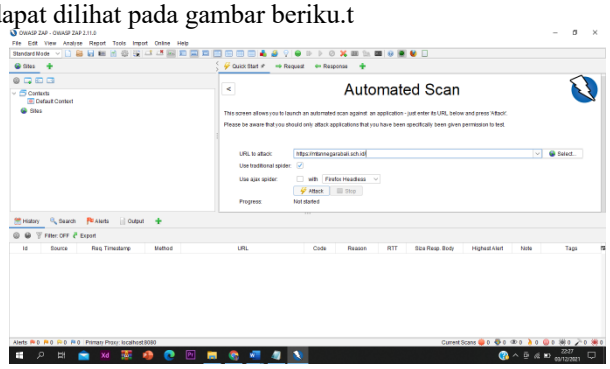
B. *Tahap Kedua*

Hasil kedua yaitu pengujian kerentanan pada Perangkat Lunak OWASP ZAP. Dengan kesesuaian langkah kedua, terlebih dahulu open tools OWASP ZAP yang sudah berhasil di instalasi. Kemudian setelah berhasil membuka *tools*, telah muncul gambar berikut ini.
Pada instruksi sistem tersebut, diperkenankan untuk memilih pilihan no dan pilih start.



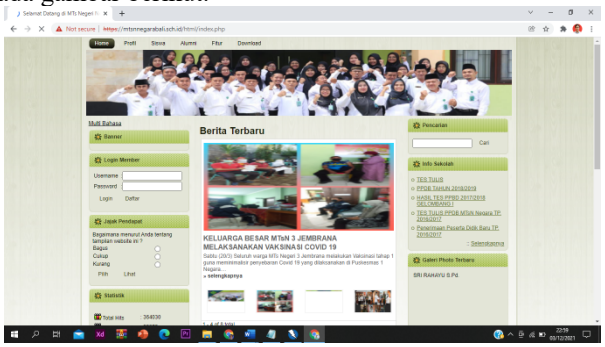
Gambar 8. Tampilan halaman utama OWASP ZAP

Untuk memulai *Scanning*; Uji kerentanan *cross-site scripting* (XSS); dan uji kerentanan *rate limiting,* melakukan *scanning* pada tools OWASP ZAP pergi ke *automated scan*. Pada tampilan ini, sudah bisa untuk memulai melakukan scanning kerentanan pada Situs Web sekolah MTsN 3 Negara, derlebih dahulu memasukkan tautan situs web ke bagian *url* to *attack*. Tampilan *attack* atau memulai *scanner* dapat dilihat pada gambar beriku.t



Gambar 9. Tampilan *attack* OWASP ZAP

Ikuti instuksi yang diberikan oleh sistem sehingga proses instalasi aplikasi berhasil dilakukan. Dengan berakhirnya tahap pertama, maka langkah-langkah berikutnya dapat dilakukan. Proses *scanner* pada situs web MTS Negeri Negara menghabiskan durasi kurang lebih 40 (empat puluh) menit lamanya. Ketika proses *scanner* ini telah dilaksanakan maka kita dapat mengetahui apa saja kerentanan yang terjadi serta level risiko dari kerentanan situs web MTsN 3 Negara yang beralamat di https://mtsnnegarabali.sch.id/. Langkah selanjutnya adalah uji kerentanan *cross-site scripting* (XSS). Pada tahap pengujian ini. Proses pertama yang dilakukan adalah pergi ke situs web MTsN 3 Negara, lebih detail ada pada gambar berikut.



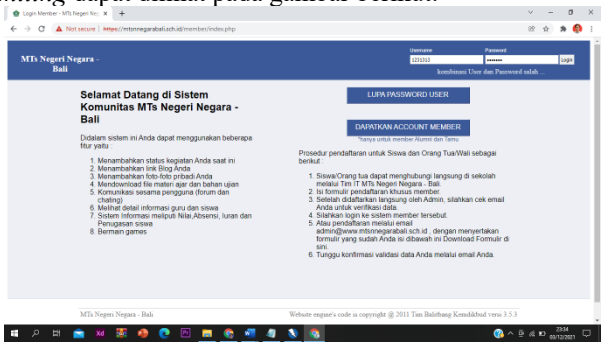
Gambar 10. Halaman beranda pada situs web MTsN 3 Negara

Gambar 10 adalah halaman beranda dari situs web MTsN 3 Negara. Terlihat pada gambar 10, bahwa ada beberapa fitur yang disediakan oleh MTsN 3 Negara pada situs web mereka. Adapun fitur-fitur yang akan diuji kali ini adalah ada pada fitur cari dan juga *login.*

Untuk melakukan Uji kerentanan *cross-site scripting* (XSS) pada situs ini, terlebih dahulu carilah salah satu kata kunci pada fitur cari di situs web di MTsN 3 Negara. Setelah masuk ke dalam kata kunci yang dicari, maka selanjutnya adalah menyisipkan salah satu dengan beberapa percobaan *payload cross-site scripting* (XSS), Kemudian mengisi pesan atau apapun sebagai penguji kerentanan *cross-site scripting* (XSS) dapat dilihat pada gambar berikut ini.

Gambar 11. Tampilan uji kerentanan *cross-site scripting* (XSS) pada situs web MTsN 3 Negara

Gambar 11 di atas merupakan proses sekaligus hasil dari uji kerentanan *cross-site scripting* (XSS) situs web MTsN 3 Negara. Adapun hasil dari uji kerentanan *cross-site scripting* (XSS) yang dapat dilihat pada gambar 11 adalah tidak ada kerentanan. Meskipun begitu, belum dapat dibuktikan bahwa situs web MTsN 3 Negara 100% aman dari serangan *cross-site scripting* (XSS). Aktivitas pengujian berikutnya adalah uji kerentanan *rate limiting.*Kerentanan *rate limiting* pada situs web MTsN 3 Negara akan berfokus kepada fitur *login* yang disediakan. Fitur *login* pada situs web MTsN 3 Negara hanya dikhususkan untuk *member* yang di antara lainnya adalah siswa, orang tua/wali siswa serta *member* yang lainnya dengan syarat mendaftar kepada tim IT MTsN 3 Negara. Namun, kegiatan penelitian kali ini telah dilakukan uji kerentanan *rate limiting* pada fitur *login*; apakah *username* dan *password* yang salah mampu mengulangi kesalahan tersebut berulang-ulang tanpa adanya peringatan *spam* atau tidak. Hasil dari uji kerentanan *rate limiting* dapat dilihat pada gambar berikut.



Gambar 12. Uji kerentanan *rate limiting* fitur *login* pada situs web MTsN 3 Negara

Pada percobaan uji kerentanan *rate limiting,* dimasukkan *username* dan *password* 1231303 sampai dengan 1231313. Dalam tiga belas kali percobaan, tidak ada peringatan

mengenai *spam login* dari sistem. Sistem hanya memberi peringatan bahwa *username* dan *password* yang dimasukkan salah. Maka dari itu, dilihat dari gambar 12; hasil dari uji kerentanan *rate limiting* pada fitur *login* adalah memiliki kerentanan. Seperti yang telah disebutkan sebelumnya bahwa situs web yang tidak memiliki peringatan *spam* di setiap percobaan *login* yang salah memiliki kerentanan pada bagian *rate limiting*.

C. Tahap Ketiga

Setelah berhasil melakukan semua tahap pengujian, maka diperlukan penyajian hasil sebagai kumpulan data pada penelitian uji kerentanan *cross-site scripting* (XSS) dan *rate limiting* pada situs web MTsN 3 Negara. Berdasarkan semua proses yang telah dijelaskan, maka dapat dikumpulkan data-data kerentanan *cross-site scripting* (XSS) dan *rate limiting* di situs web MTsN 3 Negara pada table berikut.

Tabel 1.

Tabel Hasil Uji Kerentanan Situs Web MTsN Negara

Jenis Kerentanan	URL	Risiko Kerentanan
XSS	https://mtsnneg arabali.sch.id/l ml/siswa.php? =%22%3E%3(script%3Ealert %22INI%20X S%22)%3C/sc pt%3E	Rendah
Rate limiting	https://mtsn negarabali.s ch.id/memb er/index.php	Sedang

Tabel 2.

Level Risiko Kerentanan Situs Web MTsN Negara

Angka Risiko	Risiko Kerentanan
0% < 30%	Renadh
30% < 60%	Sedang
60% < 90%	Tinggi

Risiko kerentanan dilihat dari seberapa besar celah keamanan yang terjadi pada masing-masing jenis kerentanan. Maka dari hasil uji kerentanan situs web MTsN 3 Negara telah dijelaskan secara eksplisit pada tabel 1 dengan penjelasan level risiko pada tabel 2.

D. Tahap Keempat

Tahap terakhir merupakan solusi dari hasil kerentanan yang telah ditemukan pada uji coba. Pada *cross-site scripting* (XSS), memang tidak ditemukan adanya celah keamanan yang tinggi di sana. Namun hal ini perlu tetap diwaspadai, mengingat tidak ada satupun sistem yang 100 % aman di dunia. Maka dari itu, penting untuk mempertahankan dan meningkatan keamanan dari kerentanan *cross-site scripting* (XSS). Pada risiko keamanan *rate limiting,* perlu mendapatkan perhatian khusus. Sebab dari hasil uji kerentanan ditemukan kerentanan *rate limiting* dengan risiko sedang. Solusi yang dapat dipertimbangkan lebih lanjut oleh tim pengembang atau IT situs web MTsN 3 Negara adalah merancang dan mengembangkan sistem baru pada fitur *login* yang mampu membatasi percobaan *login* lebih dari 5 (lima) kali. Selain itu, diperlukan juga fitur tambahan berupa lupa akun atau *password* yang terintegrasikan ke email *member* sehingga tidak terlalu menyulitkan proses selanjutnya. Adapun proses ini bertujuan guna mengurangi risiko akun *member* yang dibajak dengan cara memasukkan *username* atau *password* secara acak. Apalagi, saat ini pengguna internet yang menanamkan data akun mereka cenderung menggunakan *password* lumrah seperti nama tengah; tanggal lahir; angka atau alfabet yang diurut; serta *password-password* lainnya yang mudah untuk ditebak dan diacak. Batas waktu melakukan kesalahan *login* setelah lebih dari 5 (lima) juga perlu untuk diperhatikan. Sebab, ada kemungkinan juga *member* lupa terhadap *password* yang dimiliki, tetapi mereka menolak untuk mengubah *password* mereka dengan alasan tertentu.

IV. KESIMPULAN

Sudah cukup lumrah digunakan. Situs web sendiri dapat ditujukan dalam berbagai hal atau kepentingan. Salah satunya adalah bagi Lembaga pendidikan untuk menyediakan media informasi atau profil Lembaga mereka melalui situs web tersebut. Situs web atau situs serupa lainnya tidak memiliki keamanan yang dapat dikatakan 100% (seratus persen) aman dari ancaman. Oleh karena itu, OWASP ZAP menjadi salah satu tool yang dapat digunakan untuk mendeteksi kerentanan suatu situs web. Pada analisis ini, situs situs web MTsN 3 Negara menjadi bahan uji kerentanan menggunakan tools OWASP ZAP.

Berdasarkan data hasil *scan* menggunakan OWASP ZAP, situs web MTsN 3 Negara untuk menguji kerentanan XSS dan *rate limiting* situs web MTsN 3 Negara, hasil analisis OWASP ZAP untuk kerentanan XSS menggunakan playload script pada situs situs web MTsN 3 tersebut tidak memiliki celah kerentanan XSS yang cukup berarti. Lain halnya dengan analisis *rate limiting* pada situs web MTsN 3 Negara yang terdeteksi memiliki kerentanan. Kerentanannya terlihat saat tidak adanya *"alert"* saat pengguna salah memasukkan info login walau sudah berkali – kali percobaan. Hal tersebut dapat memungkinkan terjadinya pembobolan terhadap akun dengan melakukan percobaan masuk menggunakan username/e – mail dan kata sandi acak yang mudah untuk ditebak. OWASP ZAP mampu melakukan analisis kerentanan pada suatu situs web untuk menemukan celah keamanaan yang dapat di bobol dan dari hal tersebut dapat mengantisipasi kemungkinan pembobolan pada *user account*.

Antisipasi yang dapat dilakukan pada situs web MTsN 3 Negara adalah dengan mengahadirkan fitur pembatasan login lebih dari 5 (lima) kali dan fitur tambahan berupa lupa akun atau *password* yang terintegrasikan ke email *member* sehingga memudahkan pengguna apabila lupa info login akun mereka.

DAFTAR PUSTAKA

[1] Riadi, Imam, Rusydi Umar, and Tri Lestari. "Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP." JISKA (Jurnal Informatika Sunan Kalijaga) 5.3 (2020): 146-152. http://ejournal.uin-suka.ac.id/saintek/JISKA/article/view/53-02/1783

[2] Yudiana, Yudiana, Anggi Elanda, and Robby Lintang Buana. "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIKRosma Dengan Menggunakan OWASP Top 10." CESS (Journal of Computer Engineering, System and Science) 6.2: 37-43, (2020) https://jurnal.unimed.ac.id/2012/index.php/cess/article/download/24777/pdf

[3] Hidayatulloh, Syarif, and Desky Saptadiaji. "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)." Jurnal Algoritma 18.1 (2021): 77-86. https://www.jurnal.sttgarut.ac.id/index.php/algoritma/article/view/827/727

[4] Hakim, Ahmad Sultan, Triawan Adi Cahyanto, and Habibatul Aziza Al Faruk. "SERANGAN CROSS-SITE SCRIPTING (XSS) BERDASARKAN BASE METRIC CVSS V. 2." Jurnal Smart Teknologi 2.1 (2020): 54-63. http://jurnal.unmuhjember.ac.id/index.php/JST/article/view/3839